Guidelines to Design Adaptive Command and Control Structures for Cyberspace Operations

Lieutenant Colonel Jeffrey B. Hukill, USAF-Ret.

The effective command and control (C2) of cyberspace operations, as with other forms of military operations, are essential to success in the expected dynamic operating environment of the future.[1] Despite the impossibility of foolproof forecasting, there is a general consensus among studies regarding the nature of the future military operating environment. The thought is that the next 25 years will challenge military forces with threats and opportunities across the range of military operations extending from regular and irregular wars, to relief and reconstruction in crisis zones, to cooperative engagement in the global commons.[2] Confronting these threats and opportunities will require that operations are conducted in a highly integrated, networked, and distributed environment under a joint force commander. Since these operations serve a mixture of military and civil objectives, success in these operations demands the integration of capabilities from all government agencies, services, and coalition partners. Such integration stresses the need for an adaptive C2 approach for cyberspace operations built upon unified action that leads to unity of effort. [3] To guide a commander in the development of an adaptive C2 structure two key elements are needed: a clear understanding of the overall end state or goal, and identification of key variables that might influence the final design. Both of these elements were identified during an exhaustive study on C2 promoted by the United States Air Force Chief of Staff. This study on C2 was organized and conducted by the Air Force Research Institute (AFRI) at Maxwell Air Force Base, Alabama. [4] While the purpose of this article is to focus on cyberspace operations the AFRI study concluded that the C2 guidelines presented here are also applicable to all forms of military capabilities.

Goal of Adaptive Command and Control for Cyberspace Operations

The researchers conducting the C2 study analyzed recent U.S. military and humanitarian operations which are similar in nature to the expected operating environment over the next 25 years.[5] The analysis identified the following common traits needed for the development of adaptive C2 for cyberspace operations: focus on unity of effort as well as unity of command, integration of command and control functions at the lowest appropriate level, the need to create agility, and the need to enhance speed of action. Combined, these traits provide an accurate description of the overall end state or primary goal of adaptive cyberspace C2 design. The primary goal is, the creation of

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Guidelines to Design Adaptive Command and Control Structures for Cyberspace Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI) ,155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Air & Space Power Journal. Volume 24, Number 3, 2012

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

unity of effort through integration at the lowest appropriate organizational level, achieving agility and speed of action in delivering desired effects.[6]

Unity of effort stresses coordination and cooperation toward common objectives from participants not necessarily part of the same command or organization. For most missions across the range of military operations, a commander will need to integrate cyberspace capabilities that reside with other military services, interagencies, multinationals, and governments, as well as nongovernment partners. Some individuals consider such interdependence risky because success depends upon capabilities that a commander may not directly control. However, capabilities necessary to support missions across the range of military operations and the likely size and structure of the cyberspace force render this situation a reality. Commanders do not need to "own or control" partners' assets to guarantee access to their capabilities. Adaptive cyberspace C2 structures must create synergy through horizontal collaboration built on mutual trust among all war-fighting partners rather than simply emphasizing the traditional vertical interaction characteristic of the military hierarchy. Lack of trust among partners leads to the desire to "own" all assets needed for an operation; this leads to excessive control and prevents synergy. A C2 design for cyberspace operations that concentrates on unity of effort will enable a one-team, one-fight mind-set and will increase effective access to a wider range of capabilities.[7]

Another key aspect of the overall goal of cyberspace C2 involves maximizing the agility and speed of action a commander needs to decide and act quicker than an adversary. Decentralizing cyberspace operations C2 to the lowest appropriate level capable of integrating assets is the best way to increase a commander's ability to act swiftly. C2 structures inappropriately over centralized may lose agility and impair initiative, resulting in mission failure. A commander's clear guidance, intent, and priorities, as well as acceptable risk and appropriate authority for the level of responsibility, must accompany the decentralization process. Further, command relationships that enable effective horizontal collaboration between partners can enhance both agility and speed of action.[8]

The greatest challenge in achieving the goal of adaptive C2 for cyberspace operations is determining the lowest appropriate organizational level to integrate assets. In other words what is the correct balance of centralization versus decentralization within the C2 design needed to achieve unity of effort, agility, and speed of action? The actual design for attaining the goal of adaptive cyberspace C2 will vary from situation to situation. The most effective C2 design is one that is able to adjust to operational realities. A commander must understand what causes these variations or what influences the fundamental elements of C2.

Variables Impacting Cyberspace Operations Command and Control Design

David Alberts and Richard Hayes (*Power to the Edge: Command and Control in the Information Age)* describe three fundamental elements to consider

when designing any C2 structure.[9] The fundamental elements are allocation of decisions, distribution of information, and patterns of interaction. Allocation of decision rights entails giving designated individuals the authority and responsibility to make decisions between possible options, using command relationships to clearly define a commander's decision authority and responsibility. Patterns of interaction address who needs to interact (e.g., commanders, staffs, and employees), how they interact (e.g., face-to-face or by means of video teleconferences), and what types of transactions (e.g., decision, advice, and situational awareness) occur during the interaction. Distribution of information consists of the various ways and means of sharing information to inform all partners involved in an operation. It includes information sharing across service, joint, coalition, other-government, and nongovernment agencies.

Alberts and Hayes go on to say that in a perfect world the most effective way to realize unity of effort and speed of action during an operation, thus achieving the primary goal of adaptive C2 for cyberspace operations, entails decentralizing decisions, distribution of information, and encouraging interaction at the lowest organizational level.[10] In reality, however, certain variables—*common* ones and those *unique* to cyberspace capabilities—limit the complete decentralization of these three fundamental elements of command and control.

Although countless variables can influence C2 design, the key *common variables* identified across the operational examples examined in the AFRI study include; the nature of an operation, available resources, capabilities of subordinate units, degree of trust and confidence, and political risk.[11] In addition to the *common variables* the *unique capabilities* of cyberspace assets; speed, range, flexibility, and versatility, also influence the C2 design.

The level of impact from all these variables will differ according to the situation. Constant tension exists among the joint military forces' commanders during the process of determining the degree of centrally controlling cyberspace capabilities. Thus, when designing a C2 approach, a commander should assess how these items will influence an operation. Turning both the *common* and *unique capabilities* variables into a series of questions, and using the descriptions below to help answer the questions, offers a practical way of aiding commanders in the "art" of designing adaptive C2 for cyberspace operations.

What is the nature of the operation? Different operations drive different balances of centralization among the three fundamental elements. For example, global operations such as a strategic cyberspace attack generally require a high degree of centralization in order to direct mission sequencing and make adjustments during execution. Contrastingly, cyberspace operations supporting ground forces in a distributed land fight are most effective when conducted with a higher degree of decentralization, given the desire to retain tactical responsiveness. Other operations, such as computer network defense, benefit from a mix of centralization and decentralization. Centralization allows

direction of overall priorities while decentralization enables a faster tempo of operations during execution.[12]

What is the capacity of available resources versus the requirement? Simple supply and demand are significant determining factors when identifying the appropriate degree of centralization among the fundamental elements of cyberspace C2. If plenty of cyberspace assets, to include equipment and personnel, are available to deliver the desired effect, then one can highly decentralize the command and control of those assets. However, scarce resources warrant a more centralized command and control approach in order to carry out the processes used to determine the prioritization and allocation against competing requirements.[13]

Pre-established priorities of assets in limited supply but high demand, made in a centralized fashion, will allow decentralized decision makers to quickly adjust assets to execution realities. Effective prioritization permits commanders to take advantage of the unique speed, range, flexibility, and versatility of cyberspace capabilities. For example, if an event drives the need for change at the tactical level during mission execution, lower-echelon control nodes need not wait to receive higher-echelon approval to alter the cyberspace communications plan or to release limited cyberspace assets to other organizations. Effective and clearly communicated prioritization of capabilities supports decentralization of integration, improving the speed of action.

What are the capabilities of subordinate units? Other variables may allow for greater decentralization of decision authority, information sharing, and interaction but unit capabilities may not permit this form of command and control. To perform the function of command and control successfully, units must be properly organized, trained, and equipped—a process that demands clear direction concerning a unit's types of decision authority and that calls for proper development of communications infrastructure, which facilitates effective interaction and sharing of information.

What is the degree of trust and confidence among partners? Can it be changed? In general, the greater the confidence and trust among commanders, subordinates, and partners, the more likely the decentralization of fundamental cyberspace command and control elements. Trust builds confidence in others. The presence of confidence regarding the competence and actions of others encourages greater willingness to grant decision authority and share information with others. Trust is built through interaction, whereby partners must plan for that virtue and continually reinforce it. When designing a C2 approach for cyberspace operations, one must understand that trust begins with shared experiences and face-to-face interaction. In light of the perishable nature of confidence and trust, one best establishes those qualities in person, not virtually, and should take pains to guard that confidence, which is difficult to rebuild once lost.

What is the political risk? In general, C2 architecture should let frontline commanders make quick on-scene decisions, especially during the execution of complex, rapidly unfolding operations. However, as commanders and staffs build plans for operations, political considerations may dictate a more centralized approach to C2. For instance, significant political concerns could arise due to the potential for collateral damage, or creation of a strategic-level effect with cyberspace weapons would likely dictate a centralized approach. It is critical to keep such instances to a minimum. Modern information technology may entice commanders to command and control operations centrally even when those operations do not warrant such control. Despite vast improvements in technology, a single person cannot gain full situational awareness during operations with multiple, simultaneous engagements throughout a large operating area. Senior commanders must balance overall campaign execution against the pressing need for tactical flexibility. The proper equilibrium of centralization and decentralization in regards to decision authority, information exchange, and interaction should enable a subordinate's ability to support the commander's intent and meet campaign objectives.[14]

At what organizational echelon should authorities reside and where should planning and execution take place in order to exploit the speed, range, flexibility, and versatility of cyberspace capabilities? Cyberspace's *unique capabilities* require special C2 design consideration. Exploitation of the *unique capabilities*: speed, range, flexibility, and versatility leads to a more centralized approach to decision making, distribution of information, and interaction.[15] Coordinating and integrating global, theater, and subtheater operations; managing scarce assets against high demand; conducting real-time mission retasking; and simultaneously creating strategic- to tactical-level effects make a centralized approach desirable. A centralized command and control approach allows a commander to respond to changes in the operating environment and to take advantage of fleeting opportunities. The challenge for a commander is to balance the desire to centralize a C2 structure to exploit cyberspace's *unique capabilities* with the other C2 design variables. The proper balance will create unity of effort through integration at the lowest appropriate organizational level, thereby achieving agility and speed of action in delivering desired effects.

Conclusion

A commander must design a C2 structure optimized for directing, planning, and employing cyberspace capabilities to support operations that achieve an overall joint force commander's objectives all in support national security interests. To effectively operate in the emerging operating environment, modern military operations will become increasingly joint, coalition, distributed, complex, intense, and global. These conditions demand adaptive C2 of cyberspace capabilities with decision authority at the most

appropriate level of command. Creating agility to take advantage of opportunities in this dynamic environment calls for decentralization of decisions, information sharing, and interaction between commanders and staffs to the lowest appropriate organizational level capable of integrating assets. Understanding the influences on C2 design caused by the *common variables* and balancing them with the desire to exploit the *unique characteristics* of cyberspace capabilities will assist a commander in determining the lowest appropriate organizational level to push decision authority, information sharing, and interaction. At times the lowest level is at the national command level. Other times effective operations necessitate the presence of commanders having decision-making authority, possessing the required information, and interacting at organizational levels below the most senior commander—individuals who can provide optimal span of control, unity of command, and tactical flexibility. These operations also warrant distributing planners and control elements to appropriate partners' echelons and giving them information access and the authority to make decisions. Focusing on the fundamental goal of adaptable C2, and understanding, based upon the specific operation, the influence of the *common* and *unique cyberspace capabilities* will lead to effective C2 of cyberspace capabilities through flexible control, with decision authority, information distribution, and patterns of interaction centralized at the appropriate echelon of command.

Notes

1. For the purposes of this paper United States Joint Military Doctrine is used to define the terms *Cyberspace Operations* and *Command and Control*. *Cyberspace Operations* is defined as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. *Command and control* is defined as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission." Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 July 2012), 56, 80, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. The following document captures the main points from other documents that discuss the future military operating environment. While this document is from the perspective of the United States it describes operations that most countries may face. United States Joint Forces Command, *The Joint Operating Environment, 2010* (Suffolk, VA: Joint Futures Group [J59], United States Joint Forces Command, 18 February 2010), 4, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf.

3. The term *unity of effort* is defined as "coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—the product of successful unified action." The term *unified* action is defined as "the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort." Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, 2 May 2007, incorporating change 1, 20 March 2009, GL-11.

4. Research Paper 2012-5, *Air Force Command and Control: The need for Increased Adaptability,* Air Force Research Institute, Air University Press, Maxwell AFB, Alabama, July 2012.

5. The operations analyzed were *Operation Allied Force,* the Major Combat Phase of *Operation Iraqi Freedom (OIF),* the Major Combat Phase of *Operation Enduring Freedom (OEF),* the Irregular Warfare Phase of OIF, the Irregular Warfare Phase of OEF, and the Hurricane Katrina disaster relief operations.

6. A variety of lessons learned documents emphasize this idea to include United States Joint Forces Command, *Joint Operations: Insights and Best Practices*, 3rd ed. (Suffolk, VA: Joint Training Division, Joint Warfighting Center, United States Joint Forces Command, 12 January 2011), 6, https://jko.harmonieweb.org/coi/JointTrainingDivision/Documents/Insights_3rd_edition_Jan_12_2011.pdf.

7. Unites States Joint Forces Command, *Joint Operations: Insights and Best Practices* 6, 24.

8. Ibid., 6, 20.

9. David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Command and Control Research Program, 2003), 75.

10. Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*.

11. The common influences were developed from analysis of *Operation Allied Force,* the Major Combat Phase of *Operation Iraqi Freedom (OIF),* the Major Combat Phase of *Operation Enduring Freedom (OEF),* the Irregular Warfare Phase of OIF, the Irregular Warfare Phase of OEF, the Hurricane Katrina disaster relief operations, and space operations as well as from other sources, including Lt Col Clint Hinote, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?*, Research Paper 2009-1 (Maxwell AFB, AL: Air Force Research Institute, March 2009), 59–64, http://aupress.au.af.mil/digital/pdf/paper/Hinote_centralized_control_and_decentralized_execution.pdf; AFDD 1, *Air Force Basic Doctrine, Organization, and Command* 14 October 2011, chaps. 2–5, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf; and United States Joint Forces Command, *Joint Operations*, 17.

12. Hinote, *Centralized Control and Decentralized Execution*, 59–60.

13. Ibid., 61.

14. AFDD 1, *Air Force Basic Doctrine, Organization, and Command* 14 October 2011, chaps. 2–5, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf, 39.

15. For a detailed description of each of these unique characteristics, see ibid., chaps. 4 and 5; and AFDD 2, *Operations and Organization,* 3 April 2007, chaps. 1 and 2, http://www.e-publishing.af.mil/shared/media/epubs/AFDD2.pdf.

	Lieutenant Colonel Jeffrey Hukill, USAF-Ret. (BS, Norwich University; MBA, Gonzaga University; MMIS, Auburn University) joined the Air Force Research Institute (AFRI) in March 2008 and has served as chief of the Research Division, and a research professor of national security. His principal research interests include, command and control of joint forces, integration of air/ground operations, force presentation, and an effects-based approach to operations. Prior to joining AFRI, he worked as a senior military defense analyst at the Curtis E. LeMay Center for Doctrine Development and Education, teaching and writing on a variety of air and space power subjects such as the air and space expeditionary force process, antiaccess strategies, and Air Force and joint command relationships. During his 22-year Air Force career, he served in operational, command, and education positions, including assignments as installation commander, chairman of the War Theory and Aerospace Power Studies Department as well as the dean of Distance Learning at Air Command and Staff College, and a B-52G electronic warfare officer. He was the team leader and a coauthor of a Chief of Staff of the Air Force directed study titled, "U.S. Air Force Command and Control: The Need for Increased Adaptability", and coauthor of the article “Developing Flexible Command and Control of Airpower” (Air and Space Power Journal, 2nd quarter 2011). In addition, Lieutenant Colonel Hukill has contributed to a variety of other journals such as Armed Forces Journal, Defense Analysis, Joint Force Quarterly, and Air and Space Power Journal (English, Spanish, Chinese and Portuguese editions).